

Microsoft Identity and Access Strategy

Microsoft Identity and Access Strategy

Situation

- Password fatigue
- Fraud, theft, phishing, pharming
- Heightened sensitivity to privacy, tracking
- Identity recognized by CxO as top business problem
- Demand for federated applications

“Laws of Identity”

1. **Control:** only reveal information identifying user with user's consent
2. **Minimal disclosure:** solution disclosing least identifying information is most stable long term
3. **Fewest parties:** disclosure limited to parties having necessary and justifiable place in a relationship
4. **Directed identity:** must support omnidirectional and unidirectional identifiers
5. **Pluralism:** must support and channel multiple technologies run by multiple providers
6. **Human integration:** human user is component of distributed system integrated through unambiguous and safe communications mechanisms
7. **Contexts:** facilitate negotiation of mechanism between relying party and user of specific identity, while presenting consistent human and technical interface

Federated Identity Approach

- Meta-system
 - Embrace already deployed mechanisms
 - Allow evolution
- Claims-based model
 - *Claims delivered in security tokens from claims providers to relying parties*
- Be open with the industry
 - Use open protocols
 - Make implementation notes freely available

Claims

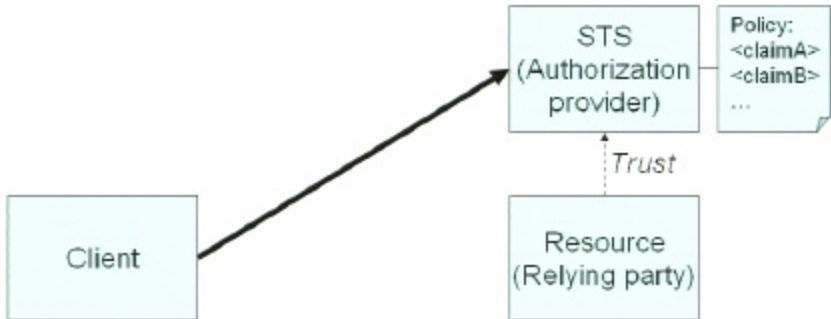
- Cryptographically verifiable information about one digital actor which another actor claims to be true
 - More than just identity assertions
- Claims transformation
 - At organizational or technical boundaries, one set of claims can be transformed into another
- Relying party specifies claims required and candidate claim providers
 - Authentication and authorization through single mechanism
- Claims delivered in security tokens (e.g. SAML) generated by Security Token Servers (STS)

Claims in WS-* Architecture



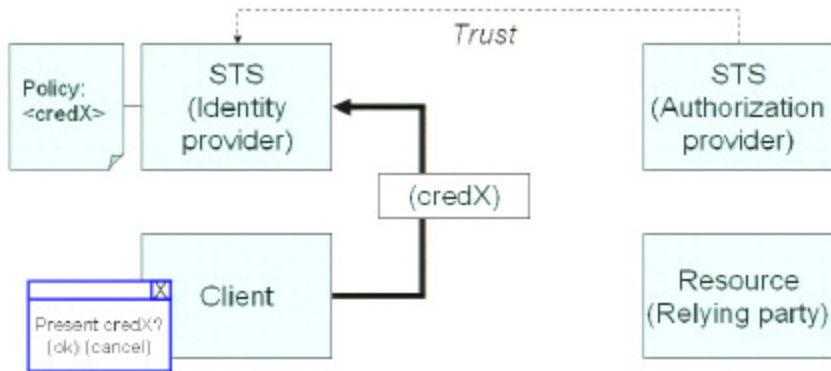
- Client to perform operation X at resource
- Client reads metadata associated with operation including policy
 - Policy indicates required claims, candidate claim providers necessary to perform operation
 - WS-MetadataExchange, WS-Policy, WS-SecurityPolicy

Claims in WS-* Architecture



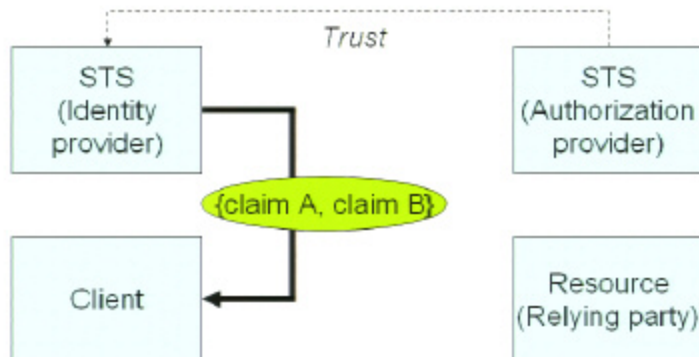
- Client requests security token with required claims from STS
 - WS-Trust
- STS policy indicates
 - Credentials necessary to obtain security token, or
 - Required claims, candidate claim providers to obtain security token

Claims in WS-* Architecture



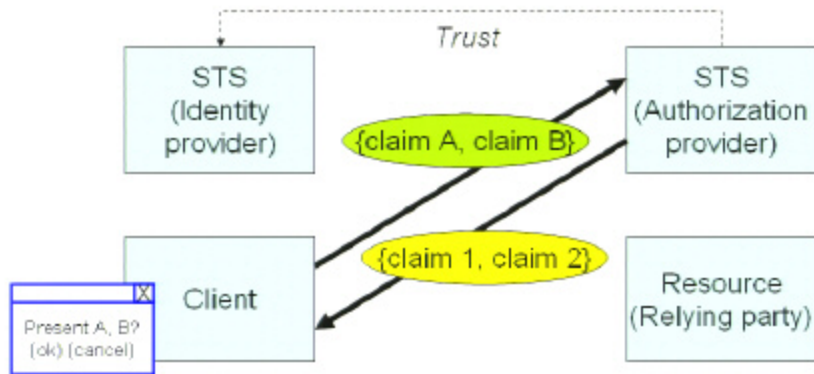
- Client requests security token from STS
- STS policy indicates credentials to obtain security token
- End user approves release of credential
- Client presents credential

Claims in WS-* Architecture



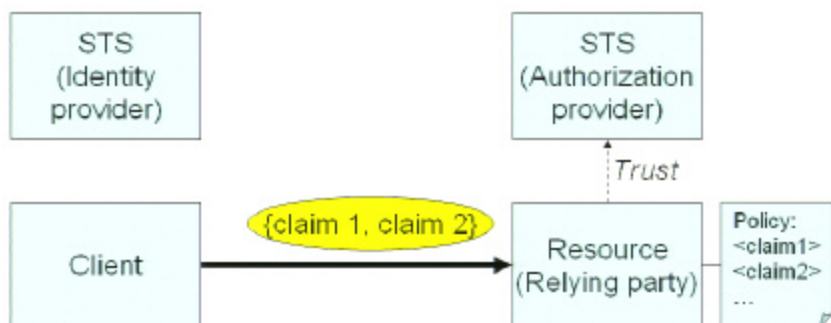
- STS returns security token

Claims in WS-* Architecture



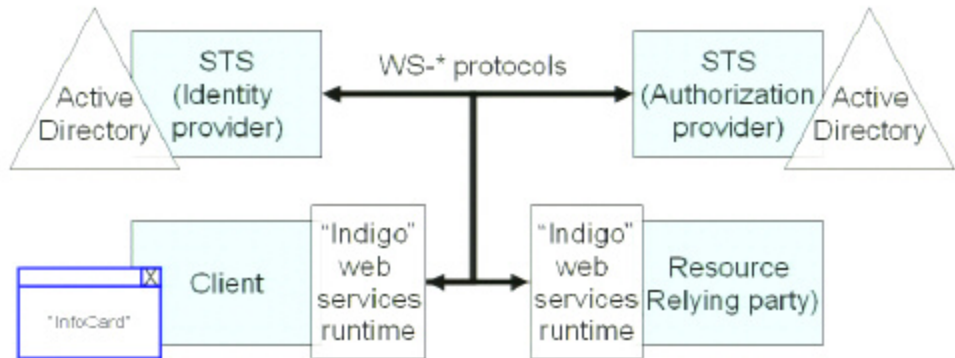
- End user approves release of claims
- Client presents security token to STS
- STS translates claims, returns security token

Claims in WS-* Architecture



- Client presents security token to resource

Microsoft Product Offering



- Active Directory-integrated Security Token Services
- "InfoCard" end user experience
- "Indigo" web services runtime for application developers
- WS-* open, interoperable protocols

“InfoCard”

- **Simple user abstraction**
 - For managing collections of claims: identity claims, membership claims, possession claims, ...
 - For managing keys for sign-in: strong computer generated keys instead of human generated passwords
- **Grounded in real-world metaphor of physical cards**
 - Gov't ID card, driver's license, credit card, membership card, ...
- **Support both self-issued and managed cards**
 - Self-issued cards signed by user
 - Managed cards signed by external authority
- **Implemented as secure subsystem**
 - Protected UI, anti-spoofing techniques, encrypted storage

Demo of User Experience

Login

Registration

DEMO OF USER EXPERIENCE
Login
Registration

DEMO

DEMO OF USER EXPERIENCE
Login
Registration

DEMO

DEMO OF USER EXPERIENCE
Login
Registration

DEMO OF USER EXPERIENCE

DEMO OF USER EXPERIENCE

DEMO OF USER EXPERIENCE
Login
Registration

DEMO OF USER EXPERIENCE

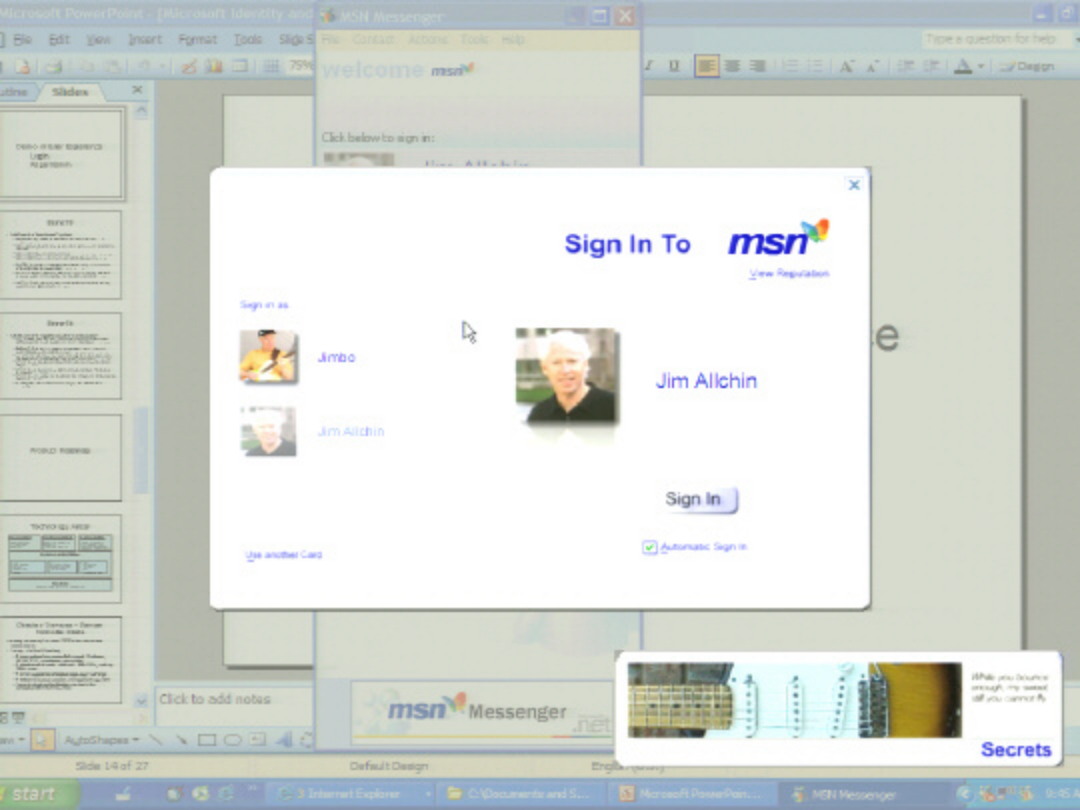
DEMO OF USER EXPERIENCE
Login
Registration

Demo of User Experience

Login

Registration

Click to add notes



Sign In To



[View Registration](#)

Sign in as



Jimbo



Jim Allchin



Jim Allchin

Sign In

[Use another Card](#)

☒ Automatic Sign in

msn Messenger



While you browse
enough, my secret
all you cannot fly

Secrets

DEMO - MSN MESSAGING
Login
MSN MESSAGING

DEMO

• MSN MESSAGING is a free instant messaging service
• MSN MESSAGING is available on Windows, Mac OS, and Linux
• MSN MESSAGING is available on the Internet Explorer, Firefox, and Netscape
• MSN MESSAGING is available on the Windows Mobile, Palm OS, and Symbian OS
• MSN MESSAGING is available on the Java, J2ME, and J2SE

DEMO

• MSN MESSAGING is a free instant messaging service
• MSN MESSAGING is available on Windows, Mac OS, and Linux
• MSN MESSAGING is available on the Internet Explorer, Firefox, and Netscape
• MSN MESSAGING is available on the Windows Mobile, Palm OS, and Symbian OS
• MSN MESSAGING is available on the Java, J2ME, and J2SE

DEMO

DEMO

DEMO	DEMO	DEMO
DEMO	DEMO	DEMO
DEMO	DEMO	DEMO
DEMO	DEMO	DEMO

DEMO

• MSN MESSAGING is a free instant messaging service
• MSN MESSAGING is available on Windows, Mac OS, and Linux
• MSN MESSAGING is available on the Internet Explorer, Firefox, and Netscape
• MSN MESSAGING is available on the Windows Mobile, Palm OS, and Symbian OS
• MSN MESSAGING is available on the Java, J2ME, and J2SE

Click to add notes

welcome.msn



Signing In...

msn Messenger



Experience

n

Timeline Slideshow X

Don't have an account?

889675

1. **Definition of "Institutional" system**
 - A system of rules and norms that governs the behavior of individuals and organizations within a society.
 - It includes formal rules (laws, regulations) and informal rules (customs, traditions).
 - It is a system of shared values and beliefs that guide behavior.
 - It is a system of shared norms and standards that guide behavior.
 - It is a system of shared values and beliefs that guide behavior.

89915

[illegible]

ROBERT ROSENBERG

[illegible]

NAME	DATE	SCORE
1. $2x + 3y = 10$	2. $4x - 5y = 20$	3. $3x + 2y = 15$
4. $5x - 7y = 35$	5. $2x + 4y = 12$	6. $3x - 6y = 18$
7. $4x + 8y = 24$	8. $5x - 10y = 50$	9. $6x + 12y = 36$
10. $7x - 14y = 42$	11. $8x + 16y = 64$	12. $9x - 18y = 72$
13. $10x + 20y = 80$	14. $11x - 22y = 99$	15. $12x + 24y = 120$
16. $13x - 26y = 156$	17. $14x + 28y = 196$	18. $15x - 30y = 225$
19. $16x + 32y = 256$	20. $17x - 34y = 306$	21. $18x + 36y = 324$
22. $19x - 38y = 380$	23. $20x + 40y = 400$	24. $21x - 42y = 441$
25. $22x + 44y = 484$	26. $23x - 46y = 529$	27. $24x + 48y = 576$
28. $25x - 50y = 625$	29. $26x + 52y = 676$	30. $27x - 54y = 729$
31. $28x + 56y = 784$	32. $29x - 58y = 841$	33. $30x + 60y = 900$
34. $31x - 62y = 961$	35. $32x + 64y = 1024$	36. $33x - 66y = 1089$
37. $34x + 68y = 1156$	38. $35x - 70y = 1225$	39. $36x + 72y = 1296$
40. $37x - 74y = 1369$	41. $38x + 76y = 1444$	42. $39x - 78y = 1521$
43. $40x + 80y = 1600$	44. $41x - 82y = 1681$	45. $42x + 84y = 1764$
46. $43x - 86y = 1849$	47. $44x + 88y = 1936$	48. $45x - 90y = 2025$
49. $46x + 92y = 2116$	50. $47x - 94y = 2209$	51. $48x + 96y = 2304$
52. $49x - 98y = 2401$	53. $50x + 100y = 2500$	54. $51x - 102y = 2601$
55. $52x + 104y = 2704$	56. $53x - 106y = 2809$	57. $54x + 108y = 2916$
58. $55x - 110y = 3025$	59. $56x + 112y = 3136$	60. $57x - 114y = 3249$
61. $58x + 116y = 3364$	62. $59x - 118y = 3481$	63. $60x + 120y = 3600$
64. $61x - 122y = 3721$	65. $62x + 124y = 3844$	66. $63x - 126y = 3969$
67. $64x + 128y = 4096$	68. $65x - 130y = 4225$	69. $66x + 132y = 4356$
70. $67x - 134y = 4489$	71. $68x + 136y = 4624$	72. $69x - 138y = 4761$
73. $70x + 140y = 4900$	74. $71x - 142y = 5041$	75. $72x + 144y = 5184$
76. $73x - 146y = 5329$	77. $74x + 148y = 5476$	78. $75x - 150y = 5625$
79. $76x + 152y = 5776$	80. $77x - 154y = 5881$	81. $78x + 156y = 6036$
82. $79x - 158y = 6199$	83. $80x + 160y = 6300$	84. $81x - 162y = 6481$
85. $82x + 164y = 6664$	86. $83x - 166y = 6849$	87. $84x + 168y = 7056$
88. $85x - 170y = 7225$	89. $86x + 172y = 7396$	90. $87x - 174y = 7569$
91. $88x + 176y = 7744$	92. $89x - 178y = 7921$	93. $90x + 180y = 8100$
94. $91x - 182y = 8281$	95. $92x + 184y = 8464$	96. $93x - 186y = 8649$
97. $94x + 188y = 8836$	98. $95x - 190y = 9025$	99. $96x + 192y = 9216$
100. $97x - 194y = 9409$	101. $98x + 196y = 9604$	102. $99x - 198y = 9799$
103. $100x + 200y = 10000$	104. $101x - 202y = 10199$	105. $102x + 204y = 10404$
106. $103x - 206y = 10609$	107. $104x + 208y = 10816$	108. $105x - 210y = 11025$
109. $106x + 212y = 11236$	110. $107x - 214y = 11449$	111. $108x + 216y = 11664$
112. $109x - 218y = 11881$	113. $110x + 220y = 12090$	114. $111x - 222y = 12321$
115. $112x + 224y = 12544$	116. $113x - 226y = 12769$	117. $114x + 228y = 13020$
118. $115x - 230y = 13225$	119. $116x + 232y = 13476$	120. $117x - 234y = 13749$
121. $118x + 236y = 14016$	122. $119x - 238y = 14221$	123. $120x + 240y = 14400$
124. $121x - 242y = 14599$	125. $122x + 244y = 14876$	126. $123x - 246y = 15069$
127. $124x + 248y = 15456$	128. $125x - 250y = 15625$	129. $126x + 252y = 15876$
130. $127x - 254y = 16081$	131. $128x + 256y = 16336$ </	

Cervine e Taurine - Cervine

- **1. Grundriss** (Grundrissplan)
- **2. Querschnitt** (Querschnittsplan)
- **3. Ansicht** (Ansichtplan)
- **4. Detail** (Detailplan)
- **5. Grundriss** (Grundrissplan)
- **6. Querschnitt** (Querschnittsplan)
- **7. Ansicht** (Ansichtplan)
- **8. Detail** (Detailplan)

Click to add notes

100

Slide 14 of 27

Default Design


English (U.S.)

start

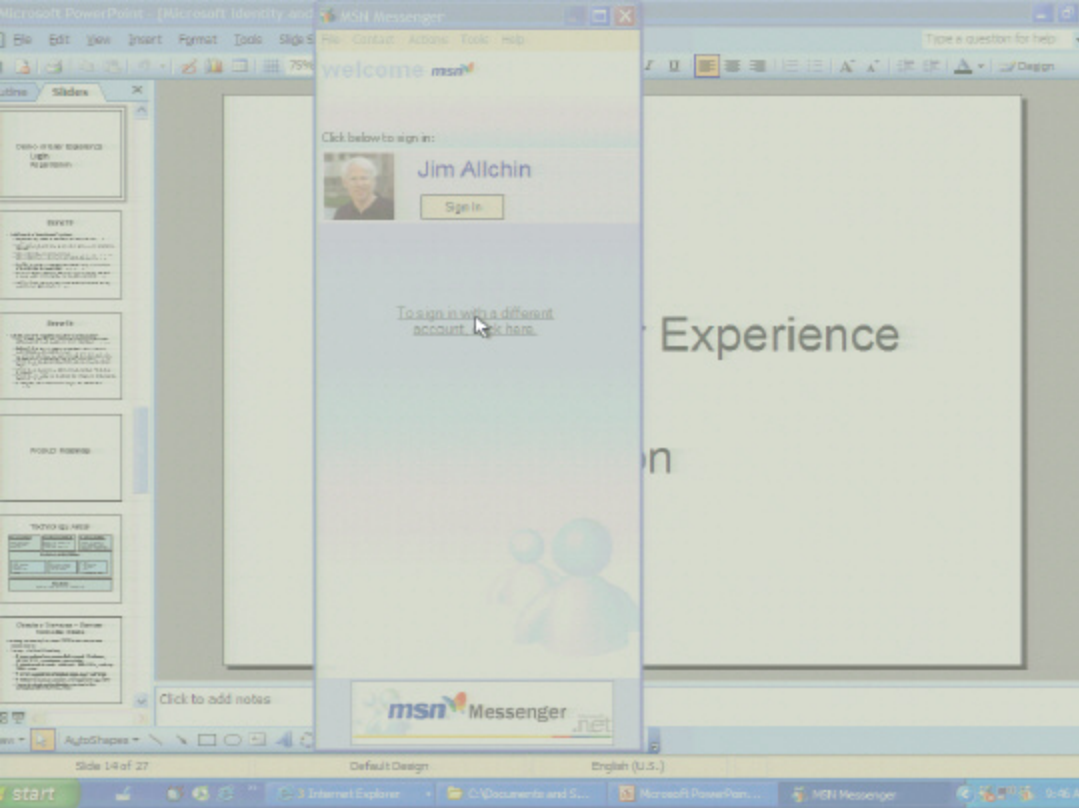
3 Internet Explorer

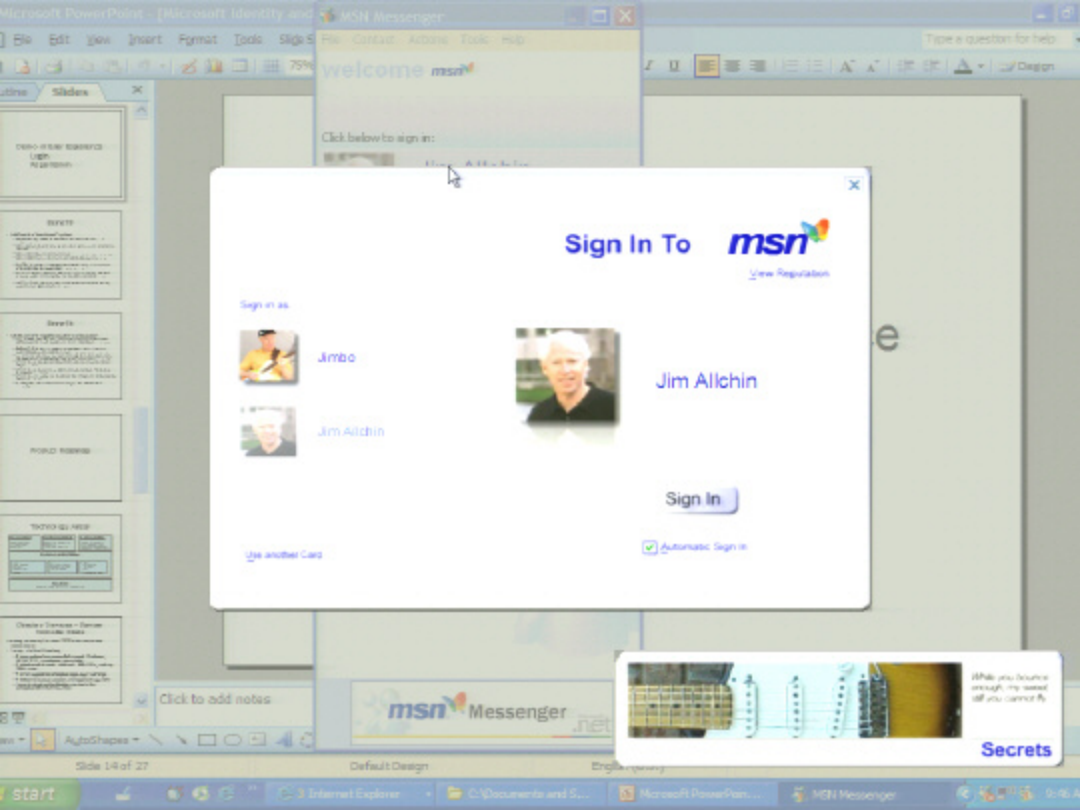
C:\Documents and S...

Microsoft PowerPoint...

 MEN Messenger

9:45 A





Sign In To



[View Registration](#)

Sign in as:



Jimbo



Jim Allchin



Jim Allchin

Sign In

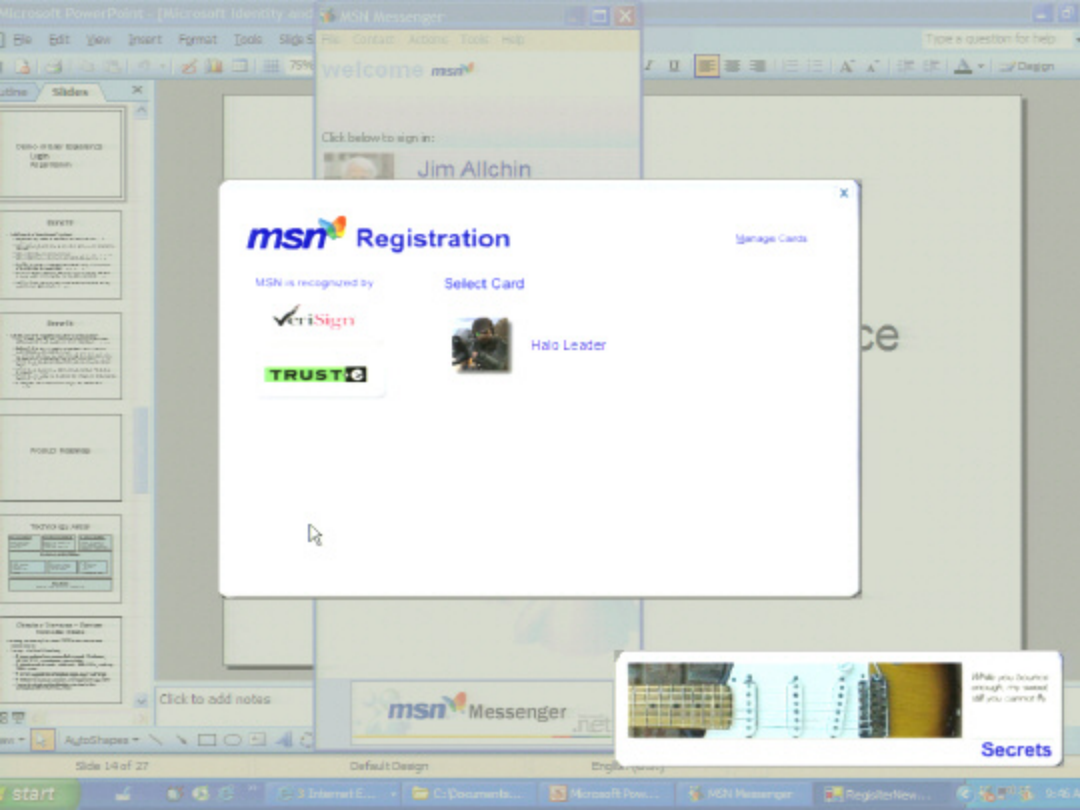
[Use another Card](#)

☒ Automatic Sign in



While you browse
enough, my secret
is all you cannot fly

Secrets



msn Registration

[Manage Cards](#)

MSN is recognized by

Select Card



Halo Leader



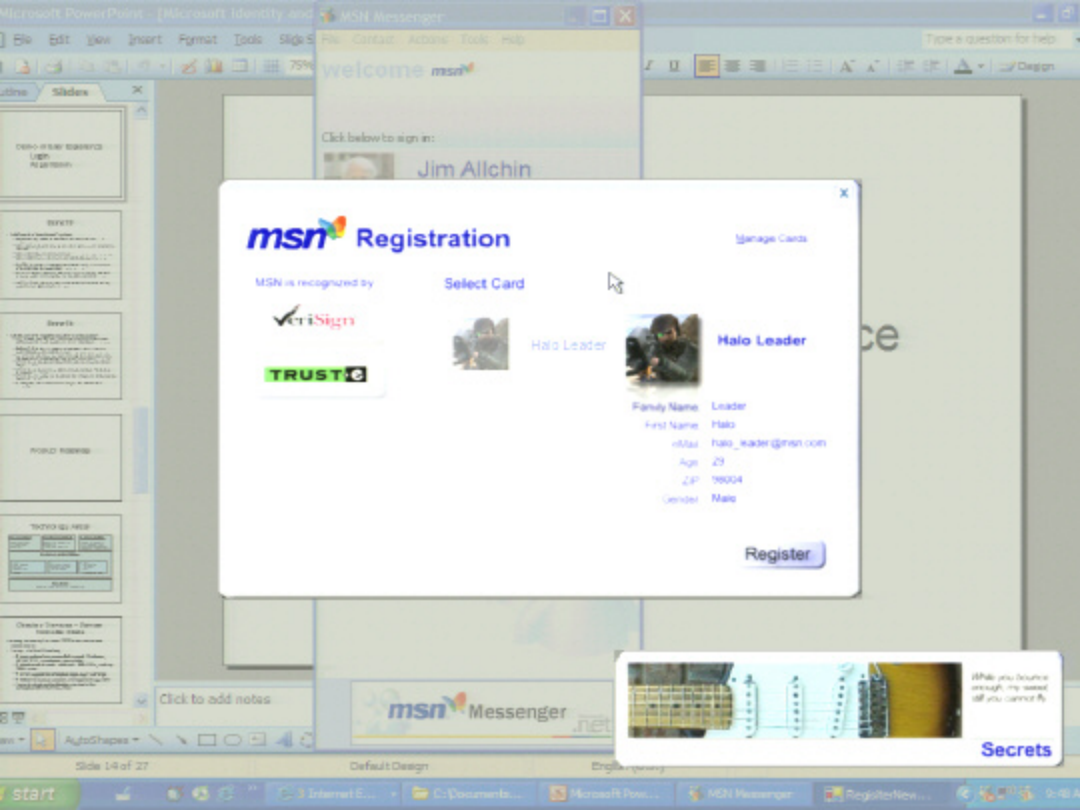
Click to add notes

msn Messenger



While you browse enough, my secret
all you cannot fly

Secrets



msn Registration

[Manage Cards](#)

MSN is recognized by

Select Card



Halo Leader



Halo Leader

Family Name	Leader
First Name	Halo
eMail	halo_leader@msn.com
Age	29
ZIP	98004
Gender	Male

[Register](#)



While you browse enough, my secret
all you cannot fly

Secrets

Product Roadmap

Technology Areas

User Experience

- Windows integration
- Office integration
- Self-Service

Developer Experience

- Directory and Identity APIs
- Access APIs
- Process integration APIs

IT Pro Experience

- Business rule authoring (e.g. provisioning rules)
- Access policy management
- Compliance, privacy reporting

Identity and Access Platform

Integration

- Synchronization
- Workflow
- Business rules
- Auditing

Directory

- Users and credentials
- Computers, services
- Policy and licenses

Access

- Web/Win SSO
- Federation
- RBAC
- Certificate Services

Connectors

Novell, Sun, IBM, Oracle, CA, SAP, PeopleSoft, Etc

Technology Areas

User Experience

- Windows integration
- Office integration
- Self-Service

Developer Experience

- Directory and Identity APIs
- Access APIs
- Process integration APIs

IT Pro Experience

- Business rule authoring (e.g. provisioning rules)
- Access policy management
- Compliance, privacy reporting

Identity and Access Platform

Integration

- Synchronization
- Workflow
- Business rules
- Auditing

Directory

- Users and credentials
- Computers, services
- Policy and licenses

Access

- Web/Win SSO
- Federation
- RBAC
- Certificate Services

Connectors

Novell, Sun, IBM, Oracle, CA, SAP, PeopleSoft, Etc

Product Roadmap

Demo of User Experience

Login

Registration

Technology Areas

User Experience

- Windows integration
- Office integration
- Self-Service

Developer Experience

- Directory and Identity APIs
- Access APIs
- Process integration APIs

IT Pro Experience

- Business rule authoring (e.g. provisioning rules)
- Access policy management
- Compliance, privacy reporting

Identity and Access Platform

Integration

- Synchronization
- Workflow
- Business rules
- Auditing

Directory

- Users and credentials
- Computers, services
- Policy and licenses

Access

- Web/Win SSO
- Federation
- RBAC
- Certificate Services

Connectors

Novell, Sun, IBM, Oracle, CA, SAP, PeopleSoft, Etc

Directory Services – Domain Controller Mode

Leading directory for host SSO and enterprise applications

- **Today: Active Directory**
 - Broad protocol and credential support: Kerberos, NTLM, SSL, smartcards, passwords
 - Performance at scale: scale out 1000+ DCs, scale up 20M+ users
 - Proven support for enterprise apps e.g. Exchange
 - Platform for secure systems management e.g. SMS
 - Trend to single authentication service in the enterprise for Unix/Linux, Mac

Directory Services – Domain Controller Mode (cont'd)

- R2
 - Unix compatibility schema
- Longhorn
 - Read-only DC: reduced physical security requirements, simplified manageability
 - Restartable AD: reduce domain controller reboots
 - DC on Server Foundation: minimize surface area
 - DC/Domain admin separation: simplified manageability

Directory Services – App Directory Mode

*Flexibility in deployment for application developers
and administrators*

- **Today: ADAM web download**
 - LDAP-only mode of AD, virtually identical code as DC mode
 - Identical performance at scale
 - Independent schema, topology, and can be sync'd with AD
 - Suitable as extranet directory, app-specific directory
 - Redistributed by multiple vendors: Oblix, OpenNetwork, etc
- **R2: ADAM included in OS distribution**
 - Built-in one-way AD-to-ADAM sync, eliminates need to deploy MIIIS/IIFP for simple scenarios
- **Longhorn: same as R2**

Access Services

Integrating federated claims-based identity and access capability into Active Directory

- Today
 - Comprehensive PKI support in platform
 - Role-based access control via Authorization Manager
 - Proven partnerships in extranet access management
- **R2: Active Directory Federation Services v1**
 - Federated web SSO
 - Interop-tested WS-Federation Passive Requestor Profile
 - Integrated with Windows SSO
 - Claims-based access model using SAML assertions
 - Federated SharePoint
- Longhorn: ADFS v1.1, AD STS, InfoCard

Integration Services

Improve security and reduce operational costs by automating and delegating identity and access management tasks

- **Today: Microsoft Identity Integration Server 2003 SP1**
 - Automate provisioning and de-provisioning
 - Enforce consistency of data across systems
 - Password management
- **R2 wave: MIIS 2003 SP2**
 - Reach: RACF/ACF2/Top Secret, SAP, Peoplesoft
 - Self service password reset

Integration Services (cont'd)

- Longhorn wave: MIIIS “Gemini”
 - Advanced workflow
 - Advanced auditing and reporting
 - Declarative policy
 - Computed memberships
 - Staff DLs, building DLs
 - Self-service platform and applications
 - “AutoGroup”

Questions and Feedback